AKILLI SAYAÇLAR KORUMA PROFİLİ
SMART METER PROTECTION PROFILE

Neslihan Güler[1], Muhammet Öztemur[1], Zümrüt Müftüoğlu[2]

1. Ortak Kriterler Değerlendirme Test Merkezi
TÜBİTAK BİLGEM
neslihan.guler@tubitak.gov.tr
muhammet.oztemur@tubitak.gov.tr

2. Ürün Belgelendirme Merkezi
TSE
zmuftuoglu@tse.gov.tr

ÖZETÇE

Son yıllarda Akıllı Şebekelerin uygulanması ve düzenlenmesi ile ilgili tüm dünya genelinde önemli gelişmeler yaşanmaktadır. Bu gelişmelere bağlı olarak, Türkiye'de de bu teknolojinin avantajlarından yararlanmak için çalışmalar başlamıştır. Türkiye Cumhuriyeti Enerji Piyasası Denetleme Kurulu ilk aşamada uzaktan okuma ve kontrol işlemlerini gerçekleştiren bir sistem önermiştir. Akıllı Sayaçlar ve bu elemanların güvenliği bu sistemin en kritik noktalarından biridir. Hazırlanacak bir Koruma Profili dokümanı ile Ortak Kriterler Standardı, bu güvenlik ihtiyacının sağlanması için uygun bir platformdur. Bu sebeple, TÜBİTAK-BİLGEM-OKTEM tarafından bir Koruma Profili hazırlanmıştır. Çalışma Türk standartları Enstitüsü (TSE) tarafından fonlanmıştır. Bu yazıda, izlenen yol haritası ve hazırlanan standart dokümanı hakkında özet bilgi verilecektir.

ABSTRACT

There have been great advancements in deployment and regulations of Smart Grid Systems all around the world throughout the late years. Following these advancements, Turkey is taking some actions to get the advantages of this technology. Energy Market Regulatory Authority (EMRA) of Republic of Turkey, suggests a system that provides metering and controlling of Smart Meters remotely in first place. Smart Meters and security of these components are the critical aspects of the system. Common Criteria Standard is a suitable platform to satisfy the security need by writing a Protection Profile. For this reason, TUBITAK-BILGEM-OKTEM has prepared a Protection Profile. The project was funded by Turkish Standard Institute (TSE). In this paper, we will give a brief description about the road map and the standard document.

1. GİRİŞ

Tüm dünyada ve ülkemizde gün geçtikçe yükselen yaşam standardı ve buna bağlı olarak artan üretim miktarı, beraberinde enerji ihtiyacını da artırmaktadır. Artan enerji talebini karşılamak için şu an kurulu olan klasik üretim ve dağıtım sistemlerini artırmak doğrudan bir çözüm gibi görünse de, bu yöntem pek çok dezavantajı beraberinde getirecektir. Üretim miktarına paralel olarak artan hammadde ihtiyacı, dağıtım sistemlerinde meydana gelen teknik kayıpların devamı, sistemin sürdürülebilmesi için ihtiyaç duyulan insan kaynağının maliyete etkisi ve çevre kirliliğinin ulaştığı tehlike sınırlarının zorlanması bunların ilk akla gelenleridir. Tüm bu nedenlerden dolayı, klasik enerji sistemlerinde yatırımların artırılması yerine, her anlamda verimliliğin artırılması esasına dayanan çalışmaların yapılması gereği ortaya çıkmıştır. Bu da akıllı şebekelerin ortaya çıkmasına zemin oluşturmuştur.

2. AKILLI ŞEBEKELER VE AVANTAJLARI

Akıllı şebekeler için literatürde birçok tanımlama mevcuttur. Akıllı şebeke kapsamının esnekliğinden dolayı, aslında bu tanımların hepsi doğru kabul edilebilir. En temel manasıyla bir Akıllı şebeke, Tesla'dan bu yana neredeyse hep aynı şekilde kullanılan klasik şebeke yapısının modern bilgisayar ve ağ teknolojileri ile entegre edilmesiyle ortaya çıkan; enerjinin üretimi, taşınması, dağıtılması ve kullanımı konusunda yeni nesil yetenekler ve teknolojik imkanlar sunan bir şebeke yapısıdır.

Akıllı şebekeler dağıtık enerji kaynakları ve diğer şebeke elemanları arasında çift yönlü bir iletişim imkanı sunarak kaynakların optimum ve verimli bir şekilde kullanımını sağlar. Akıllı şebekelerin getireceği belli başlı avantajlar şu şekilde sıralanabilir:

- Akıllı şebekelerde enerji tüketiminin uzaktan ve anlık olarak izlenip kontrol edilmesi söz konusu olduğundan, dolayı, hem tüketim verileri daha doğru olarak elde edilmekte hem de ihtiyaca göre üretim yapılarak kaynakların verimli bir şekilde kullanımı sağlanabilmektedir.
- Akıllı şebekelerde elektrik kesintisi vb. problemler daha hızlı ve doğru bir şekilde tespit edilebilmektedir. Böylece sorunların daha hızlı giderilmesi ve enerjinin kullanılamamasından kaynaklanan kayıpların önüne geçilmesi mümkün olmaktadır.
- Akıllı şebekeler, elektik üretim ve dağıtım yapısının dağıtık hale getirilmesine olanak sağlar. Bu sayede klasik şebekelerde olduğu gibi, şebekenin üretim ve dağıtım ile ilgili herhangi bir noktasında ortaya çıkacak bir problemin genel olarak tüm kullanıcıları etkilemesinin önüne geçilmiş olur.
- Akıllı şebekeler, yakın gelecekte kullanımı öngörülen akıllı cihazların (buzdolabı, klima vb.) etkin bir şekilde uzaktan kontrolü için altyapı sunar.
- Akıllı şebekeler, yenilenebilir enerji kaynaklarının dağıtık olarak üretime etkin bir şekilde katılımını sağlar. Bu sayede, başta fosil yakıtların kullanımı olmak üzere, çevre kirliliğine neden olan yöntemlerle enerji üretiminin

önüne geçilmiş olur. Ayrıca, bu yenilenebilir enerji yöntemleriyle kullanıcıların kendi elektriklerini kendilerinin üretmesi hatta ürettikleri fazla enerjiyi şebekeye satmaları mümkün olabilir. [1]

3. AKILLI ŞEBEKELERİN GÜVENLİĞİ

Akıllı şebekelerin çok yönlü olarak kontrol edilebilir ve entegre yapısının insan hayatına bir çok yenilik ve avantaj getireceği muhakkaktır. Öte yandan bu kadar önemli bir sistemde oluşabilecek bir problem, aynı ciddiyette zararlı sonuçlar doğurabilir. Akıllı şebekelerde problem oluşturmaya yönelik tehditlerin başında bu yapılara yapılacak siber-fiziksel saldırılar gelmektedir. Bu saldırılar nedeniyle çok sayıda kullanıcının elektrik kullanımından mahrum kalmasından, tüketilen elektrik miktarının yetkili makamlara yanlış iletilmesine kadar çok çeşitli sonuçlar doğabilir. Şebekeye yapılabilecek ciddi saldırılar en iyi ihtimalle çok büyük miktarda ekonomik kayba neden olacaktır.

3.1. Sayaç Güvenliğinin Önemi

Akıllı şebeke kapsamında, duyulan ihtiyaca ve sahip olunan teknolojik imkânlara bağlı olarak farklı topolojiler ortaya koymak ve hayata geçirmek mümkündür. Ancak bu uygulamalarda varlığı değişmeyen ve en yüksek öneme sahip olan bileşen daima sayaçtır. Sayaç güvenliği sağlanmamış bir sistemin güvenliğinden söz edilemez. Akıllı şebekeler ortaya çıkmadan önce de önem arz eden sayaç güvenliği konusunun akıllı uygulamalarla birlikte daha da önem kazanacağı bir gerçektir. Çünkü sayaçlar, bir enerji şebekesine ait kıymetli verilerin üretildiği ilk noktadır. Bilginin korunmasına ilişkin temel ilkelerden biri, bilginin mümkün olduğu kadar oluştuğu kaynağa yakın bir noktada koruma altına alınmasıdır. Bilginin ortaya çıktığı ilk noktada koruma altına alınması bilgiye daha sonraki noktalarda yapılacak saldırıların önüne geçebilir. Başka bir bakış açısıyla, üretildiği kaynakta koruma altına alınmayan bilginin sonraki noktalarda koruma altına alınması veya bu korumanın güvenilirliğinin sağlanması daha zor olacaktır. Örnek olarak gelişmiş bir akıllı şebeke yapısını ele alalım. Kullanıcı tüketim bilgilerinin sayaç üzerinde korunmadığını, ancak iletim hatlarındaki diğer siber tehditlere karşı güçlü önlemlerle korunduğunu düşünelim. Eğer saldırgan (bu saldırgan sayaç kullanıcısının kendisi de olabilir) sayaca erişip tüketim bilgilerinin doğruluğuna müdahale ederse, veri iletim hatları ne kadar güçlü önlemlerle korunursa korunsun, güvenli hat üzerinden merkeze üzerinde değişiklik yapılmış, yanlış veri ulaştırılacaktır. Bu örnek akıllı şebekelerdeki iletim hatlarında sağlanması gereken siber güvenliğin önemli olmadığı anlamına gelmemekte, sayaçların sistem güvenliği içerisindeki yerini vurgulamaktadır. Bağlı olduğu merkez ile uçtan uca güvenliği sağlama kabiliyetine sahip sayaçların sisteme entegresyonundan sonra, ağ güvenliği konusunda açıkta kalan noktalar analiz edilerek gerekli önlemelerin hayata geçirilmesi ile sistemin tam bir güvenliğinden söz etmek mümkün olacaktır.

3.2. Sayaç Güvenliğinde Ortak Kriterler ve Koruma Profili

Ortak Kriterler (OK), BT ürün güvenliği konusunda uluslararası geçerliliğe sahip tek standart olan ISO 15408/Common Criteria standardının dilimizdeki karşılığıdır. Bu standart, BT ürünleri/sistemleri için güvenlik gereksinimlerini ortaya koyan, bu gereksinimlerin ürün/sistemlerde gerçeklenmesi için kılavuzluk eden ve bu ürün/sistemlerin güvenlik değerlendirmelerinde esas teşkil eden bir standarttır.

OK süreci tasarım, üretim, değerlendirme ve son kullanıcıya ulaştırılma dahil olmak üzere ürünün tüm yaşam döngüsünü kontrol altına alan bir süreçtir. OK bu kontroller aracılığıyla, geliştiriciyi olası güvenlik zayıflıklarını en aza indirecek bir metodolojiye uymaya zorlar. Bahsedilen süreçlerin kontrolü ile beraber, ürüne uygulanan fonksiyonel testler ve sızma testleri (açıklık analizi) o ürün için uygun bir güvenlik garanti seviyesi verilmesini sağlar.

OK metodolojisinde önemli kavramlardan biri de Koruma Profili (PP: Protection Profile) kavramıdır. Koruma Profilleri spesifik bir teknolojide belirli ürün grubu (örn. Firewall) için özel olarak hazırlanan ve o ürün grubunun sağlaması gereken güvenlik gereksinimlerini OK çerçevesinde ortaya koyan standartlardır. Bu standartlar, o ürün özelinde sağlanması gereken güvenlik özelliklerini net ve açık bir şekilde tanımladıklarından dolayı üretici, değerlendirici ve son kullanıcı arasında ortak bir bakış açısı oluşturulmasını sağlarlar ve bir anlamda ürünün güvenlik teknik şartnamesini tanımlarlar.

OK kapsamında dünya genelinde 14 farklı ürün grubu için 254 adet PP yayınlanmıştır [2]. Farklı farklı ülkeler tarafından hazırlanan bu koruma profillerinin hiç birinin uluslararası tanınırlığı yoktur. Son yıllarda uluslararası geçerliliğe sahip koruma profillerinin oluşturulması için özel komiteler kurulmakta ve dünya çapında yoğun çalışmalar yürütülmektedir. Türkiye de gerek kendi içinde hazırladığı ulusal koruma profilleri ile gerek uluslararası çalışma gruplarına katılarak sağladığı destek ile bu standartların hazırlanması konusunda aktif bir rol üstlenmiştir.

3.3. Dünyadaki Çalışmalar

Akıllı şebeke teknolojisi dünyada her geçen gün gelişmeye devam ederken akıllı şebeke güvenliği ile ilgili çalışmalar da yoğun şekilde sürdürülmektedir. Bu konuda özel çalışma grupları oluşturularak raporlar çıkarılmakta ve düzenleyici kurumlar tarafından standartlar oluşturulmaya çalışılmaktadır. Bu kurumların başında A.B.D.'de faaliyet gösteren National Institute of Standards and Technology (NIST) kurumu ve Avrupa Komisyonu gelmektedir. NIST, 2010 yılında bu kapsamda bir seri doküman yayımlamış ve akıllı şebekeler ile ilgili güvenlik standartlarını belirlemiştir.

Ülkemiz açısından düşünüldüğünde Avrupa Birliği'nin merkezi teşkilatlarından olan Avrupa Komisyonu tarafından yürütülen çalışmalar daha çok önem taşımaktadır. Çalışmalar genel olarak akıllı şebekelerin standartlarının oluşturulması amacını taşımakta olup güvenlik konusu da bu kapsamda üzerinde çalışılan alt başlıklardan birini oluşturmaktadır. Bu kapsamda yapılan çalışmalar aşağıdaki gibi özetlenebilir.

3.3.1. M/441 EN, 12 Mart 2009

Avrupa Komisyonu tarafından; elektrik, gaz, su ve ısı sayaçlarının uyumluluğu ve standartlarının belirlenmesi amacıyla yayınlanan tebligattır. Tebligat temelde sayaçlarda çift yönlü haberleşmeyi sağlayan ve denetleyen güvenli bir

yazılım/donanım mimarisi için performans kriterleri de göz önünde bulundurularak bir standart belirlenmesini öngörür.

3.3.2. The Smart Grids Task Force (SGTF)

'Smart Grid' yapılarının verimli bir şekilde yapılandırılması amacıyla Avrupa komisyonu tarafından M/441 ve M/490 ile koordineli olarak 2009 sonunda başlatılmış bir projedir. Bu proje kapsamında hazırlanan raporlarda ürün güvenliğinin ISO/15408 Ortak Kriterler standardına göre hazırlanacak koruma profilleri ile sağlanması yönünde tavsiye niteliğinde söylemler bulunmaktadır.

3.3.3. M/490 EN, 1 Mart 2011: Smart Grid Mandate

Smart Grid Task Force kapsamında Smart Grid Information Security (SGIS), Data Protection and Privacy (DPP) ve sistemin diğer güvenlik boyutlarını belirlemek amacıyla oluşturulmuş, güvenlik konusunda daha somut isterler içeren bir tebligattır.

3.3.4. BSI Smart Meter Gateway Koruma Profili

EDeMa/e-energy (2009-2014) araştırma projesi kapsamında ilk olarak 2009 yılında başlayan bir çalışmadır. Çalışma Alman Hükümeti tarafından fonlanmıştır. Çalışma kapsamında; dağıtım şirketleri, üreticiler ve akademik gruplar yer almıştır.

Çalışma sonunda akıllı şebeke yapısı içinde akıllı sayaçların ve diğer bileşenlerin Wide Area Network (WAN)'e bağlanmasını kontrol eden "Smart Meter Gateway" modülü önerilmiştir. Söz konusu modül ve bileşenleri ile ilgili bir Koruma Profili üretilmiştir ([3], [4]). Avrupa Komisyonu çalışmaları kapsamında önerilen Koruma Profili dokümanlarının ilki olması açısından bu çalışma önemlidir. Bununla beraber; gateway üzerine yoğunlaşırken sayaç yapılarını göz ardı etmesi, çok fazla maliyet gerektirecek güvenlik özellikleri talep etmesi ve pratikte geçerliliği zor olan bazı varsayımlarda bulunması gibi nedenlerden dolayı çalışma eleştirilmektedir [7]. Tüm eleştirilere rağmen Koruma Profili isterleri uluslararası üretici firmalar tarafından dikkate alınmakta ve uyumlu ürünler üretilmektedir [8], [9].

4. AKILLI SAYAÇ KORUMA PROFİLİ

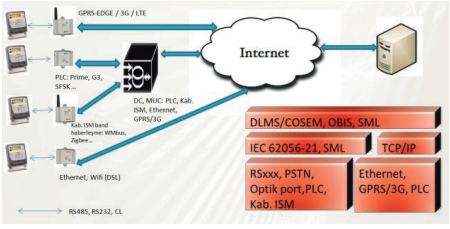
1.1. Türkiye'de Akıllı Sayaçlar ve OSOS

Ülkemizde elektrik şebekeleri için akıllı şebeke faaliyetleri OSOS(Otomatik Sayaç Okuma Sistemi) projesi kapsamında yürütülmektedir. OSOS Nisan 2011 tarihinde EPDK Tebligatı ile başlatılmış bir projedir. İlk aşamada sadece 800 MWh/yıl üzerinde tüketim yapan abonelerin kapsanması zorunludur.

OSOS sisteminin ve bu kapsamda kullanılacak elemanların asgari teknik özellikleri EPDK tarafından belirtilmiştir [5].

Söz konusu sistem incelendiğinde, uygulanmak istenen sistemin bir akıllı şebekeden ziyade gelişmiş bir uzaktan okuma sistemi olduğu göze çarpmaktadır.

Bu bakış açısıyla sistem incelendiğinde, uç noktada yer alan akıllı sayaç ve çevre bileşenleri elemanlarının kendi güvenliklerini korur ve hat güvenliğini destekler şekilde tasarlanması durumunda sistem güvenliğinin büyük ölçüde sağlanacağı anlaşılmaktadır.



Şekil 1: Türkiye'de Uygulanan OSOS Mimarisi Yapısı [10]

4.1. Koruma Profili Gerekliliği

Şu an ülkemizde kullanılan sayaçların güvenliği ile ilgili olarak, OSOS sisteminin genel mimarisini çizen tebligatta ve TEDAŞ tarafından [6] kapsamında yayınlanan asgari teknik özellikler tebliğinde bazı maddeler yer almaktadır. Her iki dokümanda yer alan güvenlik isterleri, şüphesiz belli bir tecrübenin ürünü olup büyük önem taşımaktadır. Özellikle EPDK tebligatnamesinde, OSOS sisteminde kullanılan modem modülüne başta verilerin şifrelenmesi olmak üzere ciddi güvenlik isterleri yüklenmiştir. Bununla beraber özellikle ülkemiz gibi kaçak kullanım sorununun olduğu bir yerde, güvenlik konusu fonksiyonel özelliklerden ayrı bir şekilde kapsamlı olarak ele alınması gereken bir parametredir. Bilim Teknoloji ve Sanayi Bakanlığı ve EPDK ile yapılan görüşmelerde bu durumu teyit eder nitelikte bir yargıya varılmıştır.

Öte yandan Ortak Kriterler, uluslararası ortak tanınırlığı ve BT ürün değerlendirmesinde kullanım yaygınlığı ile sayaç güvenliğinin sağlanması için uygun bir platformdur. Bu amaçla 2013 Nisan ayında TSE ve TÜBİTAK işbirliğiyle Akıllı Sayaçlar Koruma Profili hazırlama çalışması başlatılmıştır.

4.2. Koruma Profili Süreci

TÜBİTAK-BİLGEM-OKTEM (Ortak Kriterler Test Merkezi) tarafından yürütülen Akıllı Sayaç Koruma Profili hazırlanması faaliyeti kapsamında öncelikle Bilim, Sanayi ve Teknoloji Bakanlığı, EPDK gibi düzenleyici kurumlarla ve sayaç üreticileriyle görüşmeler yapılarak akıllı şebekelerin Türkiye'deki mevcut durumu çıkarılmıştır. Dünyada akıllı sayaç güvenliği kapsamında yapılan çalışmalar incelenerek bu sayaçların içinde çalıştığı sistem ile Türkiye'deki sistem kıyaslanmış, farklılıklar ve benzerlikler ortaya konulmuş ve bir yol haritası belirlenmiştir.

Bu aşamadan sonra Koruma Profili oluşturma çalışmasına başlanmıştır. İlk aşama olarak OSOS ve bunun üzerine yapılacak yenilikler ile beraber oluşacak sistemin kapsamlı bir risk analizi yapılmıştır. Bölüm 4.4'te detaylandırılan bu analizde sırası ile aşağıdaki adımlar gerçekleştirilmiştir.

- Sistem üzerinde etkisi olacak tüm taraflar tespit edilmiştir.

- Sistem üzerinde korunması gereken Varlıklar tespit edilmiştir.
- Sistemin işletilmesinde temel alınacak Varsayımlar ve Organizasyonel Güvenlik Politikaları çıkarılmıştır.
- Varlıklara yönelik tehdit oluşturabilecek saldırgan modelleri çıkarılmıştır.
- Saldırgan modelleri tarafından Varlıklara yönelik gerçekleşebilecek Tehditler çıkarılmıştır.

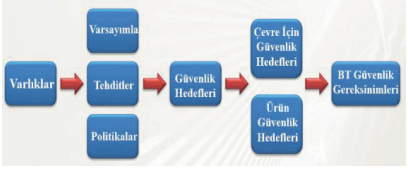
Yukarıdaki adımlar gerçekleştirilmesi esnasında toplantılar ve yazışmalar ile; Sanayi Bakanlığı, EPDK, Elektrik Sayacı Üreticileri ve Dağıtım Şirketleri ile temas kurulmuş ve görüşlerine başvurulmuştur.

Tehdit ve risklerin tespit edilmesinden sonra bu tehditleri karşılayacak bir yapının oluşturulması aşamasına geçilmiştir. Bu kapsamda:

- Sayaç elemanı tarafından sağlanması gereken güvenlik özellikleri tasarlanmıştır.
- Çevre bileşenleri tarafından sağlanması gereken güvenlik özellikleri tespit edilmiştir.

4.3. Otomatik Sayaç Okuma/Kontrol Sistemlerinin Güvenlik Analizi

Bir Koruma Profili yapısı Şekil 2'de gösterilmiştir. Güvenlik Analizi, şekilde görülen yapıda Güvenlik Hedefleri çıkarılması noktasına kadar olan kısmı kapsamaktadır.



Şekil 2 : Bir Koruma Profili yapısı

Akıllı Sayaç Koruma Profili hazırlanması kapsamında da öncelikle uzaktan okuma/kontrol sistemlerinin güvenlik analizinin yapılması gerektiği değerlendirilmiş, TÜBİTAK BİLGEM bünyesinde çalışan kripto ve ağ güvenliği uzmanları bir araya gelerek bu güvenlik risk analizini yapılmıştır. Yapılan çalışma aşağıdaki gibi özetlenebilir.

4.3.1. Sistem Kullanıcılarının Tespit Edilmesi

Uzaktan Okuma ve Kontrol Sisteminde iki tip kullanıcıdan söz edilebilir. Birincisi, Akıllı Sayaç elemanı üzerinde sahaya çıktıktan sonra ilklendirme ve işletim evresinde sayacı doğrudan kullanacak taraflardır. Bunlar:

- Akıllı Sayaç İlklendiricisi
- Veri ve Kontrol Merkezi
- Lokal Admin

Bunlara ek olarak bir de sahada iken sayacı doğrudan kullanmayıp dolaylı olarak cihazı etkileyen veya onun çalışmasından etkilenen taraflar vardır. Bunlara örnek olarak aşağıdakiler sıralanabilir:

- Akıllı Sayaç Üreticisi
- Denetleyici Otoriteler (Sanayi Bakanlığı)
- Elektrik Tüketicisi

4.3.2. Varlıkların Belirlenmesi

Öncelikle sistemde gizliliği, bütünlüğü ve kaynak doğrulaması açısından kritik olan ve sayaçta korunması gereken Varlıklar belirlenmiştir. Bunlara örnek olarak aşağıdaki taraflar sayılabilir:

- Tüketim verileri
- Merkezden sayaca iletilen kontrol komutları
- Sayaç yazılımı
- Sayaç saati

4.3.3. Varsayımların Belirlenmesi

Kritik varlıklar belirlendikten sonra sayaç ve çevre bileşenlerine ilişkin varsayımlar belirlenmiştir. Bu varsayımlara örnek olarak aşağıdakiler sayılabilir:

- Sayaç arayüzüne asıllanmış ve yetkilendirilmiş olarak bağlanan kullanıcılar güvenilir kullanıcılardır. Elde ettikleri verilere kötü amaçla veya dikkatsizlikten kaynaklı bir zarar vermeyeceklerdir.
- Denetleyiciler belli periyotlarla ve rastgele zamanlarda sayaçlar üzerinde denetimler yapacaktır. Bu denetimlerde sayacın fiziksel yapısı kontrol edilecektir.
- Akıllı sayaç modülünü üreten kişiler cihazlarda bilinçli olarak güvenlik açıklığı oluşturacak mekanizmalar eklememektedirler.

4.3.4. Saldırgan Modelleri ve Tehditlerin Tanımlanması

Belirlenen varsayımlar altında sayaca yönelik olası tehditler tanımlanırken iki türlü saldırgan tipi esas alınmıştır:

- Lokal Saldırgan: Sayaca doğrudan fiziksel erişim sağlayarak; varlıkları değiştirmeyi, elde etmeyi vb. amaçlayan saldırgandır. Sayacın kendi bölgesinde yer alan abone de lokal bir saldırgan gibi düşünülebilir.
- Uzak Saldırgan: Sayaca uzaktan/bir ağ üzerinden bağlanarak müdahale etmeye çalışan veya sayaçtan çıkan ve merkeze gönderilmeye çalışılan verilere yönelik saldırı yapabilecek saldırgan türüdür.

Bu saldırgan profilleri tarafından gerçekleştirilebilecek çok sayıda tehdit tanımlanmıştır. Bunlara örnek olarak aşağıdakiler sıralanabilir:

- Sayaçtan çıkan tüketim verilerinin Veri ve Kontrol Merkezi'ne (VKM) gönderilmesi esnasında uzak bir saldırgan tarafından araya girilerek verileri elde edebilir. Bunları değiştirerek ödenecek tüketim ücretleri üzerinden kaçakçılık yapabileceği gibi kullanıcı mahremiyetine de zarar verebilir.

- Bir Lokal Saldırgan tarafından fiziksel erişim portları üzerinden sayaca bağlanılarak sayaç üzerinde yer alan tüketim verileri üzerinde değişiklik yapılabilir.
- Veri ve Kontrol Merkezi'nden sayaca gönderilen kontrol komutları ve konfigürasyon parametreleri (tarife bilgileri gibi) bir uzak saldırgan tarafından ele geçirilerek değiştirilebilir. Böylece sayacın VKM isterleri dışında hareket etmesi (kapanması gerekirken kapanmaması vb.) sağlanabilir. Ayrıca saldırgan bu hareketiyle, sayaca istediği düşük seviyelerde ölçüm yaptırarak ödenecek tüketim ücretleri üzerinden kaçakçılık yapabilir.
- Sayacın saati bir Uzak Saldırgan ya da Lokal Saldırgan tarafından değiştirilebilir. Saldırgan bu sayede tüketim verisi ile zaman arasında yanlış bir eşleşme oluşmasına sebep olarak sayaca istediği düşük seviyelerde ölçüm yaptırabilir.
- Bir Uzak Saldırgan ya da Lokal Saldırgan tarafından, sayaç yazılımı saldırganın amacına hizmet edecek şekilde güncellenebilir. Saldırgan bu sayede sayaç üzerinde yer alan tüm varlıklara erişme ve değiştirme imkânına sahip olarak, maddi kaçakçılık ve mahremiyete yönelik saldırı gerçekleştirebilir.
- Saldırgan sayaç ünitesini açarak başta kriptografik parametreler olmak üzere gizliliği kritik olan varlıkları elde edebilir. Elde ettiği kriptografik parametreleri kullanarak sistemde yer alan güvenlik önlemlerini bertaraf ederek başka saldırılara altyapı hazırlayabilir. Tüketim verileri ve sayaç konfigürasyon parametrelerini değiştirerek ödenecek ücretler üzerinden kaçakçılık yapabilir.
- Bir Uzak Saldırgan tarafından, sayaca sürekli işlem talebi gönderilerek sayacın asli görevi olan ölçme işlemini yapması engellenebilir. Bu sayede, tüketim verilerinin düzgün bir şekilde oluşmasının önüne geçilmiş ve ödeme ücretlerinde kaçak imkânı sağlanmış olur.

4.3.5. Kurumsal Güvenlik Politikalarını Tanımlanması

Sayacın kullanımına ilişkin bir takım politikalar tanımlanmıştır. Örnek olarak aşağıdaki politika verilebilir:

- Sayaç modüllerinin fonksiyonel olarak ölçme işlemlerini düzgün bir şekilde gerçekleştirdikleri, yetkili kurumlar tarafından test edilecektir.

4.4. Güvenlik Mimarisinin Oluşturulması

4.4.1. Sayaç Güvenlik Hedeflerinin Çıkarılması

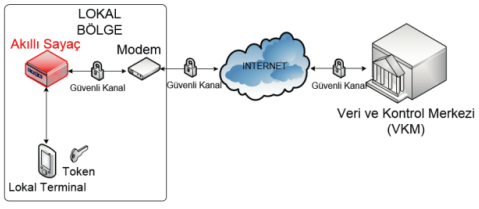
Varlıklar, varsayımlar, tehdit ve politikalar çıkarıldıktan sonra bu veriler dikkate alınarak akıllı sayaçlar için temel güvenlik hedefleri çıkarılmıştır. Bu güvenlik hedeflerine örnek olarak aşağıdakiler gösterilebilir:

- Sayaç, üzerinde taşıdığı varlıklara ve fonksiyonlarına erişim için erişim kontrolü sağlayacaktır.
- Sayaç tüketim verilerinin merkeze iletilmesi esnasında verilerin bütünlük ve gizliliğini sağlayacaktır.
- Sayaç belirli aralıklarla VKM'den aldığı bilgilerle kendi saatini güncelleyebilecektir.
- Sayaç modülünün uzaktan güvenli bir şekilde kontrol ve konfigürasyonunu yapabilmelidir.
- Sayaç, kendisine yapılan müdahaleleri zorlaştırıcı ve tespit ederek reaksiyon verici özelliklere sahip olmalıdır.
- Uzaktan güvenli bir şekilde yazılım güncelleme yapılabilmektedir.

4.4.2. Çevre Bileşenleri Tarafından Sağlanacak Güvenlik Hedeflerinin Çıkarılması

Sayacın kullanımına ilişkin bir takım politikalar tanımlanmıştır. Bunlara örnek olarak aşağıdakiler sıralanabilir:

- Gerek Veri ve Kontrol Merkezi'nden gerekse Akıllı Sayaç lokal arayüzünden Sayaca Bağlanan Kullanıcılar PIN vb. önemli verilerine sahip çıkmalıdırlar.
- Veri ve Kontrol Merkezi, kendi üzerinden Akıllı Sayaç elemanlarına bağlanacak kişilere kimlik denetimi uygulamalıdır.



Şekil 3 : Tasarlanan Türkiye Uzaktan Okuma ve Kontrol Sistemi Mimarisi

5. SONUÇ

Mevcut durum ve yakın gelecek dikkate alındığında akıllı şebekeler yolunda Türkiye'de hayata geçirilmesi planlanan sistemin bir uzaktan okuma/kontrol sistemi olduğu görülmüştür. Bu sistem baz alınarak yapılan güvenlik risk analizi ve Akıllı Sayaç elemanını temel alan güvenlik mimarisini içeren, Koruma Profili dokümanı hazırlanmıştır. [11]. Ayrıca güvenlik mimarisindeki kriptografik işlemlerin detaylarını içeren ek bir doküman hazırlanmıştır [12].

Tasarlanan güvenlik mimarisinde en temel düzeyde karakteristiği aşağıda listelenmiştir.

- Sayaç üzerinde uygulanması nispeten kolay olan simetrik kriptografik işlemler tercih edilmiştir.
- Her bir sayaç ünitesinin maliyetinin minimum düzeyde tutulmasına çalışılmıştır.
- Sayaç ünitelerinin maliyet artırımından kaçınmak için, güvenlik mimarisindeki yük Veri ve Kontrol Merkezi içerisinde yer alacak server vb. elemanlar üzerine kaydırılmıştır.

- Tasarlanan ilklendirme ve işletim süreci ile Sayacı işletecek tarafın Sayaç Üreticisinden bağımsız hale getirilmeye çalışılmıştır.
- Yapılan çalışma Akıllı Sayaç elemanı ve buna bağlı olan güvenlik standartlarını içermektedir. Sayacı yönetecek Veri ve Kontrol Merkezi'nin güvenliğinin ayrıca analiz ve kontrol edilmesi gerekmektedir.

Gelinen aşamada her ne kadar güvenlik mimarisi tasarımı ve dokümanların yazımı tamamlansa da bunlar; Sanayi Bakanlığı, EPPDK, Elektrik Dağıtım Şirketleri ve Sayaç Üreticileri'nin görüşüne sunulacaktır. Alınan geri bildirimlerden sonra dokümanlara son şekil verilecektir.

Standart dokümanların tamamlanmasından sonra, düzenleyici kuruluşlar tarafından yapılan düzenlemelerle bu standartlara uyum şartının getirilmesi ve üretilen Akıllı Sayaçların bu standartlar doğrultusunda kontrol edilmesi beklenmektedir. Bu sayede Akıllı Şebekeler yolunda ilerleyen Türkiye'nin bir geçiş kademesi olarak kurduğu Uzaktan Okuma ve Kontrol Sisteminde; Akıllı Sayaçların her türlü fiziksel ve lojik saldırılara karşı korunması, tüketimi verilerinin mahremiyet dahil güvenli bir şekilde taşınması, Sayaç elemanlarının uzaktan kontrol ve komuta edilmesi işlevlerinin güvenli bir şekilde gerçeklenmesi hedefine ulaşılmış olacaktır.

6. KAYNAKÇA

[1] Öztemür, M., Soysal, B. "Akıllı Şebekeler Yolunda Akıllı Sayaçlar", Akıllı Şebekeler Sempozyumu,2013.

[2] http://www.commoncriteriaportal.org/pps/stats/

[3] Bundesamt für Sicherheit in der Informationstechnik (BSI), "Protection Profile for the Gateway of a Smart Metering System", 2011.

[4] Bundesamt für Sicherheit in der Informationstechnik (BSI), " Protection Profile for the Security Module of a Smart Metering System (Security Module PP)", 2011.

[5] 2012 Enerji Piyasası Denetleme Kurulu, "OSOS kapsamına dahil edilecek sayaçların, haberleşme donanımının ve ilave teçhizat ve altyapının asgari teknik özellikleri", Resmi Gazete Sayı: 28105.

[6] Türkiye Elektrik Dağıtım A.Ş., "Elektronik Sayaçlarda TEDAŞ Tarafından İstenen Asgari Şartlar", http://www.tedas.gov.tr/BilgiBankasi/KitaplikMevzuatlar/Elektronik Sayaçlarda Tedaş Tarafından İstenilen Asgari Şartlar.doc

[7] Oheimb D., "IT Security architecture approachesfor Smart Metering and Smart Grid", Siemens Corporate Technology, Munich, Germany, 2012

[8] http://www.elster.com/en/press-releases/2012/1656430

[9] http://www.insys-icom.com/icom/en/energy/smart-metering

[10] Küçük Ü., "Akıllı Şebekeler: Teknolojiler Birlikte Çalışabilirlik Ve Güvenlik", Makel, ICSG, 2013

[11] Oztemur M. Guler N., "Common Crıterıa Protection Profile For Smart Meter Of Turkish Electricity Advanced Metering Infrastructure", v0.1 (draft), TUBİTAK BİLGEM, 2014.

[12] TUBİTAK BİLGEM, "Türkiye Gelişmiş Ölçüm Altyapısında Kullanılacak Akıllı Sayaçlar Güvenlik Mimarisi", v0.1 (draft), TUBİTAK BİLGEM, 2014.